WHAT IS CLAIMED:

1. A method for securing private information comprising:

calculating a first value and a second value which together are needed to derive the private information;

registering the first value with a remote server;

securely storing the second value in a local client memory that is independent of the remote server; and

deleting the first value from the local client memory.

2. The method of claim 1, wherein the private information is a private key in a public/private key pair.

3. The method of claim 1, additionally including registering an authentication value with the remote server.

4. The method of claim 1, wherein a password provided by a user of the private information is needed to derive the private information in addition to the first value and the second value.

5. The method of claim 4, wherein calculating the first and second values includes:

generating a random value;

deriving the first value from the random value; and

deriving the second value from the private information and the random value.

6. The method of claim 1, wherein calculating the first and second values includes:

generating a random value as the first value;

deriving a wrapping encryption key from the first value; and

encrypting the private key with the wrapping encryption key to form the second value.

7. A method of securing private information comprising:

entering a password;

calculating a first value and a second value and storing the first value and the second value in a local client memory, the first and second values together with the password being needed to derive the private information;

calculating an authentication value from the password;

registering the first value and the authentication value with a remote key server; and

deleting the first value from the local client memory.

8. The method of claim 7, wherein calculating the first value and the second value includes:

generating a random value;

generating a first fixed value and a second fixed value;

deriving the first value from the random value, the password, a user name, and the first fixed value; and

deriving the second value from the private information, the random value, the password, the user name, and the second fixed value;

9. The method of claim 7, wherein calculating the first value and the second value includes:

generating a random value as the first value;

deriving a wrapping encryption key from the first value, the password, and a user name; and

encrypting the private key with the wrapping encryption key to form the second value.

10. The method of claim 9, wherein the authentication value is calculated by:

generating a fixed value; and

deriving the authentication value from the fixed value, the password, and the user name.

11. A method of deriving private information of a user comprising:

receiving a first value from a key server located remotely from the user, the first value being related to the private information;

retrieving a second value stored on a computer system of the user; and

calculating the private information based on the first and second values.

12. The method of claim 11, wherein the calculation of the private information additionally includes using a password of the user to calculate the private information.

13. The method of claim 11, wherein the private information is a private key in a public key cryptographic system.

14. The method of claim 11, further comprising authenticating the user of the private information at the remote key server.

15. The method of claim 14, wherein the method of authenticating is using a biometric device.

16. A method comprising:

generating a public key and a corresponding private key for a public key cryptographic system;

calculating a first number based on the private key and a random number;

wrapping the first number using a symmetric encryption key derived from a password entered by a user of the private key; and

registering the wrapped version of the first number with a remote key server.

17. The method of claim 16, wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number

18. A computer system comprising:

a processor; and

a computer memory connected to the processor, the computer memory including a cryptographic program configured to generate a public key and a

corresponding private key for a public key cryptographic system, calculate a first number based on the private key and a random number, and wrap the first number using a symmetric encryption key derived from a password entered by a user of the private key; wherein

the wrapped version of the first number is registered with a remote server and then deleted from the computer system, the computer system retrieving the wrapped version of the first number before initiating a secure communication session using the private key.

19. The computer system of claim 18, wherein the computer memory calculates the first number by performing a logical exclusive OR of the private key and the random number.

20. The computer system of claim 18, wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number.

21. The computer system of claim 20, wherein registering the wrapped version of the first number with the remote key server further includes:

transmitting the wrapped version of the first number to the remote key server;

transmitting a user name to the key server; and

transmitting a second hash value to the key server, the second hash value being based on the password, the user name, and a second fixed random number.

22. A computer readable medium containing instructions for execution by a processor, the instructions, when executed:

generate a public key and a corresponding private key for a public key cryptographic system;

calculate a first number based on the private key and a random number;

wrap the first number using a symmetric encryption key derived from a password entered by a user of the private key; and

registering the wrapped version of the first number with a remote key server.

23. The computer readable medium of claim 22, wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number.

24. The computer readable medium of claim 23, wherein registering the wrapped version of the first number with the remote key server further includes:

transmitting the wrapped version of the first number to the remote key server;

transmitting a user name to the key server; and

transmitting a second hash value to the key server, the second hash value being based on the password, a user name, and a second fixed random number.

25. A distributed data object stored on a plurality of computers, the distributed data object comprising:

a first component, the first component being wrapped with an encryption key based on a hash value that is based on a user password, the first component being stored on a key server computer of the plurality of computers; and

a second component, the second component being wrapped with the encryption key and stored on a client computer of the plurality of computers; wherein

the first and second components of the data object, when unwrapped with the encryption key and combined using a logical exclusive OR operation, generate a private key in a public/private key encryption pair for a user of the client computer.

26. The distributed data object of claim 25, wherein the first component is calculated from the private key and the second component.

27. The distributed data object of claim 25, wherein the first component is calculated as the logical exclusive OR of the private key and the second component.

28. The distributed data object of claim 25, wherein the second component is a random number.